IHK Datenschutzbeauftragter Prüfung 2023 Praktisch

Teil A: Rechtsgrundlagen (20 P)
Aufgabe A1 (8 P)
Nennen und erläutern Sie in jeweils max. zwei Sätzen die sechs Grundprinzipien der DSGVO (Artikel 5). Je Prinzip 1,3 P.

Aufgabe A2 (6 P)
Ein Online-Händler erhebt per Kontaktformular Name, E-Mail und Bestellnummer, um Kundenanfragen zu beantworten.
a) Welcher Erlaubnistatbestand aus Art. 6 Abs. 1 DSGVO liegt vor? (2 P)
b) Nennen Sie zwei Betroffenenrechte und erläutern Sie, wie der Kunde sie im konkreten Fall wahrnehmen kann. (je 2 P)

Aufgabe A3 (6 P)
Bei einem Verstoß gegen Meldepflichten nach Art. 33 DSGVO droht ein Bußgeld in Höhe von 2 % des Weltjahresumsatzes, maximal jedoch 10 Mio EUR.
Rechnen Sie bei einem Jahresumsatz von 50 Mio EUR das Bußgeld aus und erläutern Sie kurz, warum das Ergebnis unter der Maximalbegrenzung liegt.

Teil B: Organisatorische Maßnahmen (20 P)
Aufgabe B1 (10 P)
Erstellen Sie ein Verzeichnis der Verarbeitungstätigkeiten für fünf typische Prozesse in einem mittelständischen Dienstleistungsunternehmen (z. B. Personalverwaltung, Marketing, IT-Support, Lieferantenverwaltung, Kundenbetreuung).
Skizzieren Sie in tabellarischer Form je Prozess mindestens folgende Spalten:
• Zweck der Verarbeitung
• Kategorien betroffener Personen
• Kategorien personenbezogener Daten
• Empfänger oder Empfängerkategorien
• Löschfristen

Aufgabe B2 (10 P)
Entwerfen Sie ein Schulungs- und Kontrollkonzept für Mitarbeiter zum Thema Datenschutz. Nutzen Sie eine Tabelle mit Spalten:
• Thema/Inhalt
• Zielgruppe
• Häufigkeit (jährlich, bei Änderung u. Ä.)
• Verantwortlicher
• Nachweisform (z. B. Teilnehmerliste, Quiz)

Teil C: Technische Maßnahmen (20 P)
Aufgabe C1 (10 P)
Skizzieren Sie ein Netzwerk-Diagramm (Blockschema) für den Betrieb einer Webanwendung mit folgenden Komponenten: DMZ, Webserver, Applikationsserver, Datenbankserver, interne Arbeitsplätze, Firewall, VPN-Gateway. Beschriften Sie die Zonen, Verbindungen und geben Sie an, welche Datenströme durch TLS gesichert werden müssen.

Aufgabe C2 (10 P)
Beschreiben Sie jeweils kurz und prägnant, wie Sie für die Datenbank in Aufgabe C1 die folgenden Maßnahmen technisch umsetzen:
a) Verschlüsselung ruhender Daten (3 P)
b) Pseudonymisierung von Personendaten (3 P)
c) Protokollierung und Monitoring (4 P)

Teil D: Datenschutz-Folgenabschätzung (20 P)
Aufgabe D1 (10 P)
Führen Sie eine vereinfachte Risikoanalyse durch nach der Formel R = A × S (A = Eintrittswahrscheinlichkeit, S = Schadenshöhe). Bewerten Sie für einen Cloud-Dienst zur Gesundheitsdatenverarbeitung je mit Skala 1 (gering)–5 (hoch):
• Unbefugter Zugriff (A und S jeweils bewerten, Rechnung)
• Datenverlust durch Fehlkonfiguration

Aufgabe D2 (10 P)
Erstellen Sie einen Maßnahmenplan zur Risikoreduktion aus D1. Nutzen Sie eine Tabelle mit Spalten:
• Risiko
• Maßnahme
• Wirkung (Risiko neu bewerten)
• Verantwortlicher
• Termin

Teil E: Audit & Berichterstattung (20 P)
Aufgabe E1 (10 P)
Erstellen Sie einen Auditplan für die halbjährliche Datenschutzkontrolle. Legen Sie fest:
• Auditziele
• Prüfungsbereiche
• Prüfmethoden (z. B. Interviews, Dokumentencheck, technische Tests)
• Zeitplan (Monat, Dauer)
• Verantwortliche

Aufgabe E2 (10 P)
Gliedern Sie einen Abschlussbericht über das Datenschutz-Audit in sechs Kapitel. Formulieren Sie zu jedem Kapitel in je zwei Sätzen den Inhalt.

Gesamtpunktzahl: 100 Punkte